Journal of Artificial Intelligence Practice (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2025.080109
ISSN 2371-8412 Vol. 8 Num. 1

Research on the Optimization of Intrusion Detection System Based on Artificial Intelligence

Chen Xinpeng

Hubei Minzu University, Enshi, Hubei, China

Keywords: Artificial intelligence; intrusion detection system; detection accuracy; real-time performance

Abstract: This paper discusses the application and challenges of artificial intelligence intrusion detection system in the field of network security, and puts forward the corresponding optimization countermeasures. The introduction of artificial intelligence technology to provide new solutions for intrusion detection system, but still faces challenges in various applications, for these problems using advanced AI algorithm improve detection accuracy, optimize data processing process to improve real-time, enhance system adaptability and self-learning ability and cost benefit analysis and resource optimization optimization countermeasures. The implementation of these countermeasures will help to improve the overall performance of the AI intrusion detection system and provide a more reliable guarantee for network security.

1. Introduction

With the rapid development of information technology, the problem of network security is becoming increasingly prominent, and the continuous evolution of network attack means makes it difficult for the traditional intrusion detection system to effectively deal with new threats. The introduction of artificial intelligence technology provides new opportunities and challenges for the intrusion detection system. Artificial intelligence intrusion detection system can use machine learning, deep learning and other advanced technologies to automatically extract the features of network traffic, and realize the accurate identification of potential threats. In practical application, these systems still face many challenges. This paper aims to explore the optimization countermeasures of the AI intrusion detection system to improve its overall performance and provide a more reliable guarantee for network security.

2. The importance of AI intrusion detection system optimization

2.1 The severity of network security threats

When discussing the importance of artificial intelligence intrusion detection system optimization, we have to face up to the severity of network security threats. In recent years, with the rapid development of information technology, the frequency and complexity of network attacks have shown a significant growth trend. Hackers use advanced tools and technologies to constantly find

and use system vulnerabilities to launch all kinds of network attacks. These attacks are not only difficult to prevent, but also often have a very high concealment and destructive nature. The frequent network security incidents pose a serious potential threat to individuals, enterprises and even national security. The leakage of personal information may lead to property loss and privacy infringement; enterprises will face the risk of data tampering, theft or destruction, causing economic loss and damage to credit; For national security, network attacks on critical infrastructure may lead to service interruption and information leakage, which seriously affects national security and social stability. Optimizing the artificial intelligence intrusion detection system and improving its identification and defense ability of network attacks is of vital significance for safeguarding the security of personal information, safeguarding the interests of enterprises and safeguarding the national security [1]. Through continuous technological innovation and optimization, we can respond to network security threats more effectively and build a more secure and reliable network environment.

2.2 The application potential of artificial intelligence technology in intrusion detection

The application potential of artificial intelligence technology in the field of intrusion detection is huge, especially the introduction of machine learning and deep learning technology, which significantly improves the accuracy and efficiency of intrusion detection. Traditional rule-based or signature-based detection methods are often difficult to cope with the increasingly complex and changeable network attacks, while machine learning algorithms can automatically learn and extract the characteristics of attack behavior by analyzing a large amount of network traffic data, so as to realize the accurate identification of potential threats. Deep learning technology further enhances the pattern recognition ability of the system. By building a deep neural network model, it can process and analyze complex data more efficiently, and improve the accuracy and speed of detection. AI algorithms show unique advantages in identifying unknown attack patterns. Traditional intrusion detection systems usually rely on known attack signatures or pattern libraries for matching detection, and are often inadequate for new or variant attacks. The detection system based on machine learning can use unsupervised learning and other methods to mine out abnormal behavior patterns from massive data, and can make timely and effective response even in the face of unknown attacks. This adaptability and self-learning ability enables the AI intrusion detection system to better adapt to the changing network security environment and provide strong support for network security protection.

2.3 The role of the intrusion detection system in the modern defense system

Intrusion detection system occupies a pivotal role in the modern network security defense system, is regarded as the first line of defense of network security, its key role is not only to be able to monitor real-time network traffic, timely discover and report potential security threats, more is for the subsequent prevention, detection and response work to provide crucial information support [2]. In terms of prevention, the intrusion detection system can identify and prevent the entry of malicious traffic by continuously monitoring and analyzing the network behavior, and effectively curb the occurrence of network attacks. In the detection process, the system uses advanced algorithms and technologies to accurately identify a variety of known and unknown attack modes, issue alarms in time, and provide valuable response time for the security team. In the response stage, the detailed attack information and logs provided by the intrusion detection system provide an important basis for the security personnel to take targeted defense measures, and help to quickly restore the normal operation of the system and reduce the loss.

2.4 Research background and motivation

In the current field of network security, although the intrusion detection system has been widely used, its limitations are increasingly prominent and become an urgent problem to be solved. The traditional intrusion detection system mainly relies on static rules and feature matching, and it is difficult to effectively deal with the increasingly complex and changeable network attacks, especially in the face of new attack means, the omission and false alarm rate are often high. The lack of system processing speed and adaptive ability also limits its application effect in the high flow and high concurrency environment. In view of the above limitations, this study aims to optimize the intrusion detection system by introducing AI technologies, especially advanced algorithms such as machine learning and deep learning. The aim is to improve the detection accuracy and efficiency of the system, reduce false and missing alarm, and enhance its ability to identify unknown attack mode. Through the fusion application of AI technology, it can not only improve the overall performance of the intrusion detection system, but also provide more intelligent and automatic solutions for network security defense, which has important theoretical and practical significance.

3. Optimization problems of AI intrusion detection system exist

3.1 Misreporting rate and false reporting rate

In the optimization process of artificial intelligence intrusion detection system, false alarm rate and omission rate problem has been the key factor restricting the performance improvement, the traditional intrusion detection system often depends on fixed rule base or characteristic signature matching detection, with the evolution of network attack means, the static detection method gradually exposed the defects of high false positive rate and omission rate. False positives will not only consume a lot of system resources, such as CPU, memory and bandwidth, unnecessary logging, alarm sending and event response, but also reduce users' trust in the system due to frequent error alerts, leading to resistance in practical application, and affecting the effective deployment and use of the system. Misreporting means that the system fails to detect real attacks in time, which will bring serious security risks to the network, and even cause an incalculable loss of [3].

3.2 Processing speed and real-time problems

With the rapid development of information technology, the amount of network data shows an explosive growth trend, which poses severe challenges to the processing speed and real-time performance of artificial intelligence intrusion detection system. When traditional detection systems process massive data, they often have processing delays due to the computational complexity and resource limitations, leading to the lag of detection results. This delay not only affects the system's timely detection and response to potential threats, but also is detected after the cyberattack has caused damage, missing the best defense opportunity. Real-time is one of the important indicators of the performance of the intrusion detection system, which is directly related to whether the system can respond effectively in the first time of the attack. When the real-time performance is insufficient, the system's response ability to emergency security events will be greatly reduced. When faced with complex attacks such as distributed denial of service attack (DDoS) or advanced persistent threat (APT), if the system cannot quickly identify and block the attack traffic, it will lead to serious service interruption, data leakage and other consequences. The lack of real-time may also affect the security team's tracking and analysis of aggressive behavior, increasing the difficulty of subsequent defense and response.

3.3 Insufficient adaptability and self-learning ability

In the practical application of artificial intelligence intrusion detection system, the lack of adaptability and self-learning ability has become the key problems that restrict its long-term effectiveness. With the continuous innovation and evolution of network attack means, new attack modes emerge in an endless stream, which puts forward higher requirements for the rapid adaptability of the detection system. Currently, many systems still rely on static rule libraries or feature signatures for match detection, and it is difficult to effectively deal with unknown or variant attacks. This static detection mechanism leads to the system's detection blind spots in the face of new attacks, unable to identify and respond to threats in time and accurately. The lack of self-renewal mechanism is also a major challenge facing the current detection system. In the field of network security, the development of attack means and technologies is very fast. If the detection system can not continue to learn and update its own detection ability, it will gradually lag behind the development of attack technology, leading to the lag of detection ability. This lag will not only reduce the detection efficiency of the system, but also make the system completely ineffective in the face of new attacks, bringing great risks to the network security.

3.4 Resource consumption and cost-benefit considerations

In the process of optimization and deployment of AI intrusion detection system, resource consumption and cost-benefit consideration are indispensable and important aspects. The requirement of high-performance computing is the key to improve the accuracy and real-time detection of the system, but it also brings a significant increase in the cost of the deployment of the system. In order to achieve efficient data processing and complex algorithm computing, systems often need to be equipped with high-performance servers, storage equipment and network equipment, these hardware resources procurement and maintenance costs are high, is a big burden for many organizations. With the increasing amount of data and the continuous update of algorithms, the system also needs to be expanded and upgraded regularly to meet the growing computing and storage needs of [4]. These additional inputs not only increase operating costs, but also have an impact on the stability and reliability of the system.

4. Optimization countermeasures for optimization of AI intrusion detection system

4.1 Introduce advanced AI algorithm to improve the detection accuracy

In order to improve the detection accuracy of artificial intelligence intrusion detection system, the introduction of advanced AI algorithm is feasible optimization countermeasures, deep learning model, such as convolutional neural network (CNN) and recurrent neural network (RNN), because of its powerful feature extraction and pattern recognition ability, in reducing false alarm and omission has significant advantages. Through the effective combination of convolution layer and pooling layer, CNN can automatically learn and extract the deep features in the network traffic data to realize the accurate identification of potential threats. RNN is good at processing sequence data, which can capture the time dependence in network traffic and further improve the accuracy of detection. Integrated learning method is also an effective way to improve the overall performance of the system. By combining the prediction results of multiple base classifiers (such as decision tree, support vector machine, etc.), integrated learning can make full use of the advantages of each classifier and improve the robustness and generalization ability of the system. In the intrusion detection system, the integrated learning method can not only reduce the false and missing reports

caused by a single classifier, but also improve the ability of the system to identify the unknown attack mode by integrating the detection results of different classifiers.

4.2 Optimize the data processing process and improve the real-time performance

In order to improve the real-time performance of the AI intrusion detection system, optimizing the data processing process is the key, and it is crucial to design efficient feature extraction and data preprocessing strategies. By adopting advanced feature selection algorithms and preprocessing techniques, such as standardization and normalization, the data dimension and noise can be effectively reduced, the data quality can be improved, and more accurate and effective input can be provided for the subsequent algorithm model. The distributed computing framework is also an effective means to improve the speed of large-scale data processing. By splitting data processing tasks into multiple sub-tasks and performing them in parallel on multiple computing nodes, the distributed computing framework can make full use of computing resources and significantly improve the efficiency of data processing. In the intrusion detection system, this means that the system can analyze the network traffic data faster, identify and respond to potential threats in time, and enhance the real-time performance of the system.

4.3 Enhance the system's adaptability and self-learning ability

To enhance the artificial intelligence intrusion detection system adaptability and self-learning ability, realize the model based on online learning update mechanism is the core strategy, through continuous monitoring network traffic data, and automatically trigger the new threat model update, the system can quickly adapt to the changing attack mode, keep the advancement and detection ability effectiveness. The development of continuous optimization strategy based on feedback cycle is also an important way to improve the evolutionary ability of the system. By comparing and analyzing the system detection results with the actual situation, feedback data is formed and the model is iteratively based on these data, the detection accuracy and robustness of the system can be continuously improved. This continuous optimization mechanism not only helps the system to adapt to new threats in time, but also can accumulate knowledge and experience in the continuous learning process, and improve the overall performance of the system.

4.4 Cost-benefit analysis and resource optimization

In the deployment and operation of artificial intelligence intrusion detection system, cost-benefit analysis and resource optimization are the key to ensure the sustainable operation of the system. In order to reduce resource consumption and improve the economy of the system, the adoption of lightweight model and hardware acceleration technology has become an important strategy [5]. Lightweight models, such as the streamlined network structure based on deep learning, can significantly reduce the computational complexity and memory footprint, and reduce the input of hardware resources while maintaining high detection accuracy. Combined with hardware acceleration technology, such as GPU parallel computing, dedicated integrated circuit (ASIC), it can further improve the data processing speed, reduce energy consumption, and achieve efficient utilization of resources. In terms of the deployment scheme, the hybrid architecture based on cloud computing and edge computing provides new ideas for balancing performance and cost. The cloud computing platform provides powerful computing power and storage resources, can handle large-scale data sets, and supports the operation of complex algorithms. In edge computing, the deployment of computing nodes on the edge of the network, realizes the nearby processing and analysis of data, reduces the data transmission delay, and improves the real-time performance of the

system. Combining the advantages of the two, an intrusion detection system can meet the high performance requirements and effectively control the cost. By dynamically adjusting the resource allocation and optimizing the task scheduling, the system can flexibly adjust the computing and storage resources according to the actual situation, so as to realize the efficient utilization of the resources and the effective control of the cost.

5. Conclusion

This paper deeply analyzes the application of the AI intrusion detection system in network security and proposes corresponding optimization countermeasures. By introducing advanced AI algorithms, optimizing the data processing process, enhancing the system adaptability and self-learning ability, and conducting cost-benefit analysis and resource optimization, the detection accuracy, real-time, adaptive ability and economy of the artificial intelligence intrusion detection system can be significantly improved. The implementation of these optimization countermeasures will help improve the overall performance of the system and provide more comprehensive and reliable protection for network security.

References

[1] Zhou Mengmeng. Research on the design of communication network intrusion detection system Based on Artificial Intelligence [J]. Information recording materials, 2023, 24 (12): 192-194.
[2] Yao Hong. Design of communication network-intrusion detection system Based on artificial intelligence [J]. Network Security and informatization, 2023 (9): 54-56.
[3] Shen Rongrong. Design of computer network intrusion detection method based on artificial intelligence technology [J]. Yangtze River Information and Communication, 2023, 36 (5): 127-129.
[4] Tan Qinhong, Tian Yingxin. Design of communication network-intrusion detection system Based on artificial intelligence [J]. Yangtze River Information and Communication, 2022, 35 (12): 189-191.
[5] Yuan Xiaogui. Application of artificial intelligence system in communication network intrusion detection technology [J]. Information and Computer, 2023, 35 (9): 176-178.